CRYPTREC Report 2016

平成 29 年 3 月

独立行政法人情報処理推進機構

国立研究開発法人情報通信研究機構

CRYPTREC-RP-0003-2016

「暗号技術活用委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構によって共同で運営されている暗号技術活用委員会の 2016 年度活動報告である。

暗号技術活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。2015 年度に、暗号技術活用委員会の活動目的の軸足を、「暗号技術を主軸とした検討」から「情報システムのセキュリティ確保に寄与する暗号技術等に係る成果物の提供」に移すことに定義し直し、2016 年度から新たな目的に基づいて活動を開始した。

2016 年度の暗号技術活用委員会では、利用者に使いやすい運用面でのガイドライン（運用ガイドライン）を本格的に整備していくことを今後の活動の中心に据えることを視野に入れ、暗号プロトコルに関する部分については暗号プロトコル課題検討 WG にて検討し、それ以外の部分については暗号技術活用委員会にて、CRYPTREC として扱うべき運用ガイドラインの対象について検討を行った。2017 年度以降の活動においては、運用ガイドラインの必要性や目的、書かれるべき内容や想定読者、作成時に考慮しなければならない課題、参考にすべき他組織が発行したガイドラインや連携すべき関連組織について 2016 年度に整理した検討結果を踏まえて、有益な運用ガイドラインを優先的かつ効率的に作成していく所存である。

さらに、運用ガイドラインは、ガイドライン作成時の標準化状況や製品状況、利用環境や利用実績等を踏まえて作成時における現実的かつ効果的な推奨設定や推奨基準を提示するものであることから、ある程度の時間が経過し、それらの状況が変化すれば、運用ガイドラインの中身も陳腐化し、ガイドラインとしてふさわしくないものとなる。そこで、運用ガイドラインの質を維持するためのアップデートのあり方について検討を行い、例えば 2015 年に公開した「SSL/TLS 暗号設定ガイドライン」について、昨今 SSL/TLS に関する状況が大きく変化していることを反映して 2017 年度にアップデートする予定とするなど、今後運用ガイドラインの整備を進めるにあたっての方針を取りまとめた。

今年度の活動成果をもとに来年度以降、運用ガイドラインの拡充を図っていくことが、ひいては情報システムのセキュリティ確保の底上げ、暗号の普及促進・セキュリティ産業の競争力強化に繋がり、より安心・安全な情報化社会の実現に結び付くことを期待している。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

暗号技術活用委員会 委員長　松本 勉

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI[1] システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、2016 年度の暗号技術活用委員会の活動内容と成果概要を記述した。

2015 年度以前の CRYPTREC Report は、CRYPTREC 事務局（総務省、経済産業省、国立研究開発法人情報通信研究機構、及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトから参照できる。

http://www.cryptrec.go.jp/report.html

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号技術活用委員会（以下「活用委員会」）は、図 1 に示すように、総務省と経済産業省が共同で運営する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（IPA）と国立研究開発法人情報通信研究機構（NICT）が共同で運営している。

活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。

2016 年度は、2015 年度に定めた活動計画に基づいて活用委員会の活動を開始した。活用委員会では 2017 年度以降、運用ガイドラインの作成を開始するため、運用ガイドラインの対象範囲等について検討を行い、特に暗号プロトコルについては暗号プロトコル課題検討 WG にて検討した。

なお、活用委員会と連携して活動する「暗号技術評価委員会（以下「評価委員会」）」も暗号技術検討会の下に設置され、IPA と NICT が共同で運営している。

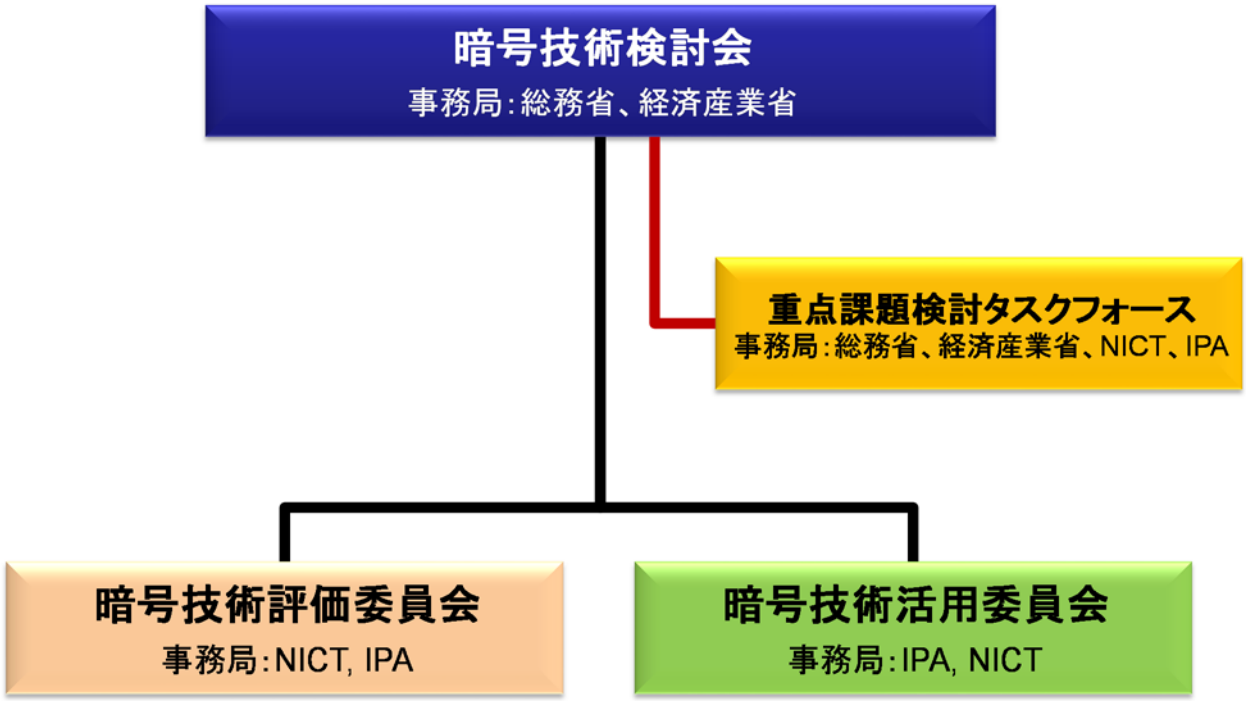

図 1　2016 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

委員長	松本 勉	横浜国立大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	菊池 浩明	明治大学 教授
委員	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	杉尾 信行	株式会社 NTT ドコモ
委員	清藤 武暢	日本銀行
委員	手塚 悟	慶應義塾大学 特任教授
委員	寺村 亮一	NRI セキュアテクノロジーズ株式会社 主任
委員	松本 泰	セコム株式会社 ディビジョンマネージャー
委員	三澤 学	三菱電機株式会社 主席研究員
委員	満塩 尚史	内閣官房 政府 CIO 補佐官
委員	村木 由梨香	日本マイクロソフト株式会社 セキュリティプログラムマネージャー
委員	山岸 篤弘	一般財団法人日本情報経済社会推進協会 主席研究員
委員	山口 利恵	東京大学 特任准教授
委員	渡邊 創	国立研究開発法人産業技術総合研究所 企画主幹

暗号プロトコル課題検討ワーキンググループ

主査	菊池 浩明	明治大学 教授
委員	大泰司 章	一般財団法人日本情報経済社会推進協会 室長
委員	坂根 昌一	シスコシステムズ合同会社 エンジニア
委員	佐古 和恵	日本電気株式会社 技術主幹
委員	佐藤 直之	SCSK 株式会社 シニアプロフェッショナルコンサルタント
委員	下山 武司	株式会社富士通研究所 主管研究員
委員	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	清藤 武暢	日本銀行
委員	寺村 亮一	NRI セキュアテクノロジーズ株式会社 主任
委員	村木 由梨香	日本マイクロソフト株式会社 セキュリティプログラムマネージャー
委員	吉田 博隆	国立研究開発法人産業技術総合研究所 主任研究員
委員	渡辺 大	株式会社日立製作所 主任研究員

オブザーバー

内田 稔	内閣官房内閣サイバーセキュリティセンター[2016 年 10 月まで]
久保山 拓	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター

眞弓 隆浩　　内閣官房内閣サイバーセキュリティセンター
森安 隆　　内閣官房内閣サイバーセキュリティセンター[2016 年 9 月まで]
赤谷 俊彦　　総務省 行政管理局[2016 年 8 月まで]
廣田 亮　　総務省 行政管理局
筒井 邦弘　　総務省 情報流通行政局[2016 年 6 月まで]
上東 孝旭　　総務省 情報流通行政局[2016 年 7 月から]
丸橋 弘人　　総務省 情報流通行政局
今野 孝紀　　総務省 情報流通行政局
加藤 誠司　　経済産業省 産業技術環境局
上坪 健治　　経済産業省 商務情報政策局
希代 浩正　　経済産業省 商務情報政策局[2016 年 6 月まで]
中野 辰実　　経済産業省 商務情報政策局[2016 年 6 月まで]
中村 博美　　経済産業省 商務情報政策局[2016 年 6 月まで]
森川 淳　　経済産業省 商務情報政策局[2016 年 7 月から]
松本 裕悟　　防衛省 整備計画局
吉岡 達宏　　防衛省 整備計画局
岡野 孝子　　警察大学校
多賀 文吾　　警察大学校
相原 大輔　　警察大学校

事務局

独立行政法人情報処理推進機構（江口純一、時田俊雄、小暮淳、神田雅透、稲垣詔喬、兼城麻子）
国立研究開発法人情報通信研究機構 （宮崎哲弥、能見正、盛合志帆、野島良、吉田真紀、
大久保美也子、篠原直行、黒川貴司、金森祥子）

2016 年度の活動内容と成果概要

1. 活動内容

2015 年度に、「CRYPTREC の在り方に関する検討グループ」及び「重点課題検討タスクフォース」での検討結果に基づき、暗号技術活用委員会での活動方針の軸足を、「暗号技術を主軸とした検討」から「情報システムとしてのセキュリティ確保に寄与する成果物の提供」に移し、新たな活動方針を以下のように定義し直した。

【活動目的】

暗号技術活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として必要な活動を行うものとする。具体的には、実運用とセキュリティ確保の両面の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント

2016 年度は、上記の活動目的を踏まえ、運用面でのマネジメントに関するガイドライン（以下、運用ガイドライン）を本格的に整備していくことを今後の暗号技術活用委員会（以下、活用委員会）での活動の中心に据えることを視野に、以下の項目について検討を行った。

① 作成すべき運用ガイドラインの対象及び取扱い範囲の切り分けの検討
② 作成した運用ガイドラインのメンテナンス体制の検討
③ 外部組織や業界団体との連携方法の検討
④ 運用ガイドラインの作成
⑤ ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保する利用価値の高い成果物となるようにコントロールする
⑥ その他
CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、「暗号プロトコル課題検討 WG（以下、課題検討 WG）」を設置

なお、①については、暗号プロトコルに関わる部分を課題検討 WG で、それ以外の範囲を活用委員会でそれぞれ検討した。また、④と⑤については、実際の運用ガイドラインを作成する際に、テーマに応じて適切な手段を活用委員会で判断して実施していくことになった。

2. 今年度の委員会の開催状況

2016 年度暗号技術活用委員会は 2 回開催された。各回会合の概要は表 1 のとおり。また、暗号プロトコル課題検討 WG は 3 回開催された。各回会合の概要は表 2 のとおり。

表 1　2016 年度暗号技術活用委員会　開催概要

回	開催日	議案
第 1 回	2016 年 11 月 9 日	・暗号プロトコル課題検討 WG 活動状況報告 ・運用ガイドライン（「SSL/TLS 暗号設定ガイドライン」）のメンテナンス方法に関する検討 ・運用ガイドラインの対象範囲に関する検討
第 2 回	2017 年 3 月 15 日	・暗号プロトコル課題検討 WG 活動報告 ・暗号プロトコル以外の運用ガイドラインの対象の検討 ・外部連携の進め方の検討 ・2016 年度暗号技術活用委員会報告書

表 2　暗号プロトコル課題検討 WG　開催概要

回	開催日	議案
第 1 回	2016 年 10 月 27 日	WG 活動概要の説明、課題についての自由討議
第 2 回	2016 年 12 月 26 日	第 1 回 WG での討議を踏まえた課題の整理と更なる検討
第 3 回	2017 年 2 月 10 日	報告書案の取りまとめ

3. 成果概要

3.1. 運用ガイドラインの対象について

2017 年度以降に活用委員会として運用ガイドラインを作成する価値がある対象を検討するにあたっては、以下の目的と領域に合致する範囲のガイドラインを想定して議論を行った。なお、暗号設定ガイドラインのうち、暗号プロトコルに関する部分については課題検討 WG にて検討を行い、それ以外の部分については活用委員会にて検討を行った。

- どのような目的をもつ運用ガイドラインにするか
  1. 現在利用されている仕組みの中で安全ではない使われ方を排除し、安全性の底上げを図る（NIST SP800 シリーズのような推奨設定の基準（ガイドライン）をイメージしたもの）
  2. 利用者が理解しやすく、かつ採用しやすいベストプラクティスを示す（NIST SP1800 シリーズのような利用しやすいガイドをイメージしたもの）

3. 普及が進んでいない安全な仕組みの普及・活用を促進させる（安全な仕組みへの移行を促すようなガイドをイメージしたもの）
4. 政府、業界団体等が守るべき（半）強制的基準として示す（そうなるような環境整備を含む）

- どのような領域の運用ガイドラインにするか

A. 暗号設定ガイドライン
  - 開発実装に関連するガイドライン
  - 暗号利用・運用・設定に関連するガイドラインで暗号プロトコル以外のもの
  - 暗号利用・運用・設定に関連するガイドラインで暗号プロトコルに関するもの
  - 特定の製品・サービスを安全にするために関連するガイドライン

B. マネジメント関連のガイドライン
  - 暗号システムの運用マネジメントに関連するガイドライン

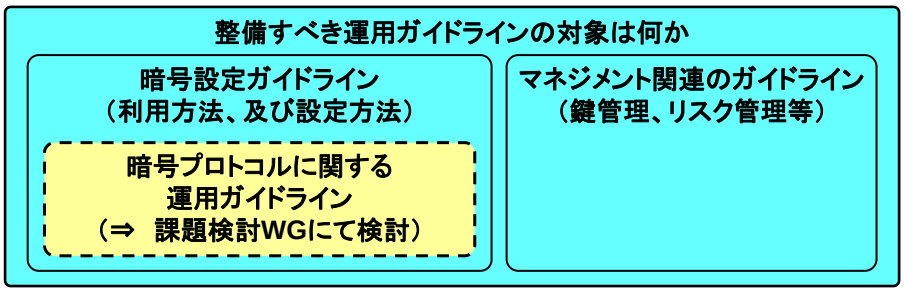

図 2　整備すべき運用ガイドラインの対象及び取扱い範囲の切り分け

【暗号プロトコルに関する運用ガイドライン以外の対象】

もともと運用ガイドラインの必要性が高いと考えられている対象を中心に、以下の観点から整理を行った。

表 3 に検討結果をまとめる。今後、運用ガイドラインを作成していく際には、表 3 に挙げたもののなかから優先的に取り上げていくことが望ましい。なお、「課題」には CRYPTREC が作成する運用ガイドラインの価値を高めるために考慮しなければならないポイントをまとめており、また「関連組織」には連携先として有効と期待される国内組織（国際組織の日本支部を含む）を記した。活動計画の立案に当たっては、これらのポイントを踏まえた計画であることが望まれる。

- 【対象】
  どのような用途で使う運用ガイドラインであるか
- 【目的・内容】
  どのような目的をもった運用ガイドラインを意図したものか（3.1 で挙げた目的の 1. ～4. のどれに当たるか）

- 【内容】
  運用ガイドラインに記載される内容はどのようなものか
- 【想定読者】
  その運用ガイドラインの想定読者は誰か
- 【必要性】
  なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

なお、表 3 の「領域」列、及び「目的」列の表記についての注意は次のとおりである。

●「領域」列について
・開発実装に関連する文書類
・暗号利用・運用・設定に関連する文書類で暗号プロトコル以外に関するもの
・暗号システムの運用マネジメントに関連する文書類
・特定の製品・サービスを安全にするために関連する文書類

●「目的」列の表記の意味
①・・・現在利用されている仕組みの中で安全ではない使われ方を排除し、安全性の底上げを図る（安全性評価を含む）
②・・・利用者が理解しやすく、かつ採用しやすいベストプラクティスを示す
③・・・普及が進んでいない安全な仕組みの普及・活用を促進させる
④・・・政府、業界団体等が守るべき（半）強制的基準として示す（そうなるような環境整備を含む）

表 3　取りまとめ結果一覧

領域	No	対象	目的	内容	想定読者	必要性（※委員から意見）	ガイドライン作成にあたっての課題	他組織が発行したガイドライン等	関連組織
開発実装	1	鍵管理（生成・保管・削除）の実装	① ②	・乱数性テストのチェック項目 ・安全な鍵生成方法 ・鍵の保管 ・鍵の削除	・システム開発者（特に、プログラマー）、運用者 ・今後システムを構築する中小企業 ・製品開発者	・他の対象に比べて、「鍵管理」を優先的に検討してほしい。 ・鍵の元となる技術であるため、重要（特に公開鍵暗号の鍵生成）。不適切な実装では、知らないうちに素因数を他の鍵と共有している事例もある。 ・日本の情報セキュリティ対策の底上げになる。暗号を応用（利用）したシステム全般の参考にもなる。 ・システム開発者や運用者が想定読者になりうるかは定かでないが、製品開発者向けには必要。 ・SP800-90 では、乱数に必要なエントロピー等について言及しているが、実際には最低限どのようにすればよいのかがわからない。特に、リアルタイム性を要する鍵についてどこまでやればよいかがわかるものがほしい。	・書くべきことの範囲が広い。 ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難。 ・鍵管理に関する規格を網羅的に調査する必要がある。 ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成	SP800-90A, B, C	
	2	サーバ証明書の検証方法	①	アプリにおけるサーバ証明書が適切に検証されるための実装方法	システム開発者(特に、アプリケーション開発者)	・アプリでのサーバ証明書検証不備の脆弱性が多い。 ・IoT 向けに、大量、高速、省リソースという様な観点で、サーバ証明書の検証方法だけでなく、PKI の構築全般について策定されれば、組込機器向けにも参考になる。			
	3	電子署名・検証実装方法	① ② ③	システムに電子署名や検証アプリを実装する方法（ネイティブアプリを作る場合やマルチプラ	システム開発者	・システムへの電子署名や検証アプリの実装者向け文書が少ない。今までは Java でブラウザプラグインとドライバーとをつないでいたが、Java がブラウザプラグインをサポートしない	・実装方法が、技術依存する可能性があり、時		JNSA 電子署名 WG

				ットフォームを想定したブラウザベースの場合等）		方針が表明されており、様々な実装が出てくることが予想されるため、実装に関する情報が必要。 ・民間企業が、JPKI の署名検証を行うことができるようになったので、民間企業のアプリにおいても、電子署名を行うアプリを実装することが現実化してきた。 ・実装方法を示さないと多くのアプリが開発されず、電子署名が普及しない。普及のために、実装方法をレクチャーするものという位置づけである。 ・従来は専門家が電子署名の実装を行っていたが、今後は専門ではない SIer も実装に携わる可能性があるため、電子署名を適切に実装させるために必要である。	期によって変化する。 ・実装方法が複数ある。		
開発 実装	4	Captcha の検証方法	① ②	・各社勝手に導入している Captcha の最低限の安全性検査 ・過度に利便性を下げていないか	システム開発者（特に、アプリケーション開発者）	・各社様々な方式で導入している。銀行などのウェブサイトへのログインにも多用されている。 ・チャレンジレスポンスだと考えれば、必ずしも暗号に無関係ではないため、ガイドラインがあるとよい。			
	5	将来の暗号危殆化対策を見据えたシステム設計・開発方法 ※C．暗号システムの運用マネジメントにも記載	②	将来の暗号危殆化対策を見据えたシステム設計・開発方法 －インシデント対応方針 －暗号アルゴリズムの切替(代替) －当該暗号の使用停止　等	システム設計者、開発者（運用者）	・今後開発されるシステムにおいて、暗号危殆化対応の観点から、設計段階で考慮すべきことを明確化・明文化する必要がある。 ・2030 年頃に使用を停止する 112bit 安全性の暗号に対する危殆化対策は、時期尚早であるため、他のテーマに比べて、優先度は低い。 ・ただし、これから IoT や組み込みなどが普及してくるため、2030 年ぎりぎりまでやらなくてもよいというわけではない。	・一般的な留意点は整理可能である一方、利用しているシステム毎に暗号の使い方が異なるため、具体手にガイドするのは難しい。		

						・暗号をカセッタブルに実装することが必要であり、それをガイドする必要がある。			
暗号利用・運用・設定（暗号プロトコル以外）	6	鍵管理（生成・保管・削除）の設定/運用	① ② ③	・鍵管理（生成・保管・削除）上の要求事項 ・代表的な製品での具体的な設定方法例（BitLocker, Azure Key Vault 等）	・システム開発者（例えば、プログラマー）、運用者 ・今後システムを構築する中小企業	・暗号を利用するうえで、鍵を秘密に保つことが重要であるにも関わらず、IT 担当者の中には鍵がどういうものかを知らない人すらいる状況であるため、普及啓発が必要。 ・他の対象と比べて「鍵管理」を優先的に検討してほしい。 ・日本の情報セキュリティ対策の底上げになる。暗号を応用（利用）したシステム全般の参考にもなる。 ・鍵管理について個別の製品ごとの設定例が必要である。 ・データ処分(Data Disposed)にも関連する鍵の削除についても必要。 ・例えば、SQL, Exchange といったアプリケーションや、Active Directory での証明書を利用した認証、Federation での認証などを含めると証明書および鍵の管理が必要となる対象が大規模に存在する。 ・ファイル暗号、ディスク暗号に関しても同様に大規模な対象がある。EFS 暗号化、BitLocker（あるいはデバイス暗号化）の利用率は年々高まっている。	・書くべきことの範囲が非常に広いため、対象範囲を絞る必要がある。 ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難。 ・鍵の生成・削除の文書と併せて用意ができるとよい。 ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成。	・安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン（案） ・SP 800-57 Part 2 ・SP 800-57 Part 3 Rev. 1	IPA

暗号利用・運用・設定（暗号プロトコル以外）	7	SSL・SSH の鍵管理	① ②	・OpenSSL の鍵管理 ・CSR を作るときのパスワードの設定	システム管理者、運用者	・他の組織で作成していないようであれば、作成できるのが望ましい。	他組織ですでに存在するようであれば、作成する必要がない。		IPA
	8	ドキュメントへの署名	① ③	・PDF の暗号化/署名における暗号の設定	PDF 利用者	・PDF への署名ということでガイドラインがあるべき。PDF の署名で利用する証明書には SHA-1 が利用されている例もあり、適切に利用させる必要があるので、ガイドを作成するべき。 ・署名なしの PDF を出している人も多いため、署名をさせるべき。 ・ユーザが不正な署名に気が付かないので、ユーザへの啓蒙が必要。 ・検討範囲を明確化する必要があるため、時期尚早。代替手段（ファイル暗号化ソフトや Cloud 環境）も存在しており、すぐに対応しなければならないわけではないため、優先度は低い。	・PDF にいくつものバージョンがあり、互換性など懸念。 ・ドキュメント管理というと PDF だけでなく、PDF だけでも製品数が多い。 ・日本では主に JNSA が署名について、検討しているため、JNSA との相談（連携）が必要。		JNSA
	9	保管データ (Data at Rest)	④	・保管データにおける暗号化方法 ・保管データ暗号化における鍵管理	システム開発者、運用者	・「高度な暗号化」の定義が明確に定まっていないため、明確にした文書（ガイドライン）があるとよい。 ・保管データを暗号化する方法についての文書（や基準）がないため、個人情報保護ガイドラインから参照できるような文書が必要。暗号について議論できる組織体が CRYPTREC しかないので、作成すべき。 ・法律的に定められる必要があり、民間では実施が困難であるため、CRYPTREC で作成するのが望ましい。	他の組織でも検討しているため、歩調を合わせた基準とするためにもリエゾンを組みながらやらなければならない。	NIST SP800-111	個人情報保護委員会

暗号利用・運用・設定（暗号プロトコル以外）	10	データの処分 (Data Disposed)	④	暗号鍵破棄による暗号化された情報の処分についての考え方や方法	システム開発者、運用者	・暗号化を利用して、機密情報を破棄する方法についての文書（や基準）が日本にはないため、個人情報保護ガイドラインから参照できるような文書が必要。CRYPTREC は国内で暗号について議論できる組織体の代表であるため、検討すべき。 ・Cryptographic erase がベストプラクティスであり、法律上認められないとデータの破棄が大変になるので、非常に困るため、検討すべき（例えば、バックアップテープの破棄）。	他の組織でも検討しているため、歩調を合わせた基準とするためにもリエゾンを組みながらやらなければならない。	NIST SP800-88 Rev.1	個人情報保護委員会
	11	使用中のデータの暗号化 (Data in Use)	②	・暗号化されたまま情報を利用することについての考え方や方法	システム開発者、運用者	・NIST にもガイドラインはないため、検索可能暗号等高機能暗号のガイドラインが必要。	他の組織でも検討しているため、歩調を合わせた基準とするためにもリエゾンを組みながらやらなければならない。		
暗号システムの運用マネジメント ※考え方・思想を含む	12	鍵管理（生成・保管・削除）の考え方	① ③	・鍵管理の考え方 ・鍵生成・管理・削除のライフサイクル ・人がどのように運用するかという手続きも含む	・システム開発者（例えば、プログラマー）、運用者 ・今後システムを構築する中小企業	・暗号を利用するうえで、鍵を秘密に保つことが重要であるにも関わらず、IT 担当者の中には鍵がどういうものかを知らない人すらいる状況である（普及啓発も必要）。 ・まずは考え方をまとめたものを作るべきなので、鍵管理関係の中で、優先的に取り組むべき。 ・鍵管理の考え方が整理されていれば、暗号を応用（利用）したシステム全般の参考にもなるため、日本の情報セキュリティ対策の底上げになる。 ・すでに、2010 年度版リストガイド（鍵管理）があるため、参考にする、もしくはアップデートするといった方法も視野に入れ、検討すべき。	・技術的な観点だけでなく、法制度を考慮して作成すべき。 ・書くべきことの範囲が広い。 ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難。 ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成。	・NIST SP 800-57 Part 1 Rev. 4 ・NIST SP800-130A	

	13	暗号システムデザイン	① ② (③)	・システム内で利用する暗号機能のマッピング（全体像） ・ネットワークのゾーニングと暗号機能の関係 ・ユースケース別の暗号の使いどころを示す（SSL/TLS 暗号設定ガイドラインの上位レイヤのドキュメントとして位置づけ） ・効果的な使い方と効果的でない使い方の例示	システム開発者（特にSIer）、運用者、プログラマー等	・例えば、得られる費用対効果が大きくないにも関わらず、SSL 通信と IP-VPN を利用した 2 重の暗号化を実施する、機密性を確保できる範囲を意識せず、SSL アクセラレーターを配置するなど、ユーザ及び SIer は暗号対策をどこまでどのように実施すればよいかわからないため、暗号機能を含めたネットワーク設計パターンを示す文書が必要。 ・システムとして、適切なコストでセキュリティを確保するための指針が必要。	・システム構成のサンプル種類がとても多いため、網羅的に書くのは難しい。 ・効果的でない使い方をバッドプラクティスとして検討するのは難しい。		
暗号システムの運用マネジメント ※考え方・思想を含む	14	将来の暗号危殆化対策を見据えたシステム設計・開発方法 ※A. 実装開発にも記載	②	将来の暗号危殆化対策を見据えたシステム設計・開発方法 －インシデント対応方針 －暗号アルゴリズムの切替(代替) －当該暗号の使用停止　等	システム設計者、開発者（運用者）	・今後開発されるシステムにおいて、暗号危殆化対応の観点から、設計段階で考慮すべきことを明確化・明文化する必要がある。 ・2030 年頃に使用を停止する 112bit 安全性の暗号に対する危殆化対策は、時期尚早であるため、他のテーマに比べて、優先度は低い。 ・ただし、これから IoT や組み込みなどが普及してくるため、2030 年ぎりぎりまでやらなくてもよいというわけではない。 ・暗号をカセッタブルに実装することが必要であるため、ガイドする必要がある。	一般的な留意点は整理可能である一方、利用しているシステム毎に暗号の使い方が異なるため、具体的にガイドするのは難しい。		
	15	RSA から楕円曲線暗号への移行	① ③	RSA から楕円曲線暗号への移行の推進	システム設計者、開発者（運用者）	・暗号技術は移行が必要となるので、移行を促進するガイドラインを作成する必要がある（さしあたっては、特に RSA から楕円曲線暗号）。 ・PKI が最も影響を受ける。			

						・暗号の移行には時間がかかるため、RSA から楕円曲線暗号への移行について、早々に整理する必要がある。			
特定の製品・サービス	16	クラウドにおけるセキュリティメカニズムの比較調査	① ②	・クラウドが採用している暗号化の対象・方式・設定をサービスごとに列挙（秘密計算、秘密分散も含む） ・クラウドサービスにおける TLS で利用している暗号化方式 ・ストレージの暗号化方式 ※定期的に調査を実施するのが好ましい	企画者、システム開発者（特に SIer）	・ユーザがクラウド利用時も暗号に注意して利用するために必要。 ・統一基準でも、クラウドの利用に関しては、クラウドのセキュリティを確認することになっているが、現状では個別に暗号方式や設定等を確認することが困難。	・サービス提供者が情報を開示してくれるかは不明。 ・そもそもガイドラインではなく、調査報告書になる可能性がある。	JIS Q 27017	CSA（Cloud Security Alliance）

【暗号プロトコルに関する運用ガイドラインの対象】

暗号プロトコルに関する運用ガイドラインの対象を検討するにあたっては、「(STEP1) 検討対象とする暗号プロトコルの列挙」と「(STEP2) 列挙した暗号プロトコルのなかから運用ガイドラインを作る価値がある／必要性が高いと判断したものを抽出」の 2 段階で議論を行った。

(STEP1) 検討対象とする暗号プロトコルの列挙

課題検討 WG では、暗号プロトコルの列挙にあたって、以下の観点から整理を行った。
その結果、表 5 にまとめる暗号プロトコルが検討対象として列挙された。

- 【種類】どのような性質のガイドラインが必要と考えられるか

表 4　ガイドラインの種類

ガイドラインの種類	ガイドラインの概要例	状況
安全性評価に関するガイドライン	• 安全性のお墨付きをつけたプロトコル（＝CRYPTREC 暗号リストのプロトコル版） • 評価されていないプロトコルに対する安全性方法 • 安全なプロトコルを設計するためのガイドライン	• 特定目的のために多くのプロトコルが提案されている • 暗号の専門家が関与しないでプロトコルが作られており、安全性評価が不十分 • 標準化を待っていられないため、先行して実装が進んでいる
実装・開発に関するガイドライン	• 製品の安全な実装・開発をするためのガイドライン • 安全な実装であることを検証するための基準	• この種のガイドラインがない • 各社独自の実装になっている
設定に関するガイドライン	• 製品に実装されている設定方法を適切に設定して安全に利用するためのガイドライン	• プロトコルレベルよりも製品レベルのほうが需要がある • 仕様が固まっている低レイヤのプロトコルであれば、運用ガイドラインが作りやすい

- 【対象】どのようなところで使われる暗号プロトコルを対象範囲とするのがよいか

Web／証明書失効管理／DNS／NW 管理／鍵管理／ユーザ管理／ユーザ認証／デバイス認証／バイオメトリクス暗号／ID 連携／無線通信／近距離通信／IC カード／メール／リアルタイム通信／ファイル共有／ファイル転送／リモート接続／VPN／自動車／制御システム／仮想通貨／放送暗号

表 5　検討対象となりうる暗号プロトコルの列挙一覧

（「★」がついているプロトコルは暗号に直接関係がないもの）

種類	対象	プロトコル名称
安全性評価（暗号技術評価委員会への参考意見とする）	ID 連携	・OpenID Connect
	無線通信	・LoRaWAN
	近距離通信	・Zigbee
		・Bluetooth
	仮想通貨	・Bitcoin プロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）
実装／開発	近距離通信	・NFC ・Felica ・ISO/IEC14443 TypeA，TypeB
	IC カード	・Felica
	自動車	【車内】CAN，CAN FD，LIN，FlexRay 【車外】DSRC，ETC2.0 【ハードウェア】EVITA 【センサ】空気圧センサ、ミリ波レーダー
	制御システム	・PLC ・SCADA

種類	対象	プロトコル名称
設定／運用	バイオメトリクス暗号	・テンプレート保護 ・FIDO
	ID 連携	・OpenID Connect ・SAML
		・OpenID Connect（HTTPS 上で利用） ・代理認証
		・SAML（HTTPS 上で利用） ・代理認証
	無線通信	・WEP ・WPA ・WPA2
	近距離通信	Zigbee
		Bluetooth
	メール	・DKIM ・SPF★ ・DMARC★
	メール	S/MIME を利用したメール送信（メールへの署名）

設定／運用	Web	・QUIC
		・HTTP/2★
	証明書 失効管理	・CRL ・OCSP
	DNS	・DNS ・DNSSEC （DANE,DPRIV を含む）
	NW 管理	・SNMP ・NETCONF ・UPnP
	鍵管理	・KMIP
	ユーザ管理	・RADIUS（EAP-TLS 等の利用を含む） ・PAP★ ・CHAPv2 ・IEEE802.1X
		・LDAP★ (kerberos)
	ユーザ管理	・PAP★ ・CHAPv2
		・TESLA
	ユーザ認証	・二要素認証

設定／運用		・パスワードつき Zip を添付したメール送信 ・S/MIME を利用したメール送信（メールの暗号化） ・オンラインストレージサービス
	メール	OpenPGP を 利用したメール送信
		・POP3 ・SMTP ・IMAP （－/over SSL/ with SASL)
		・メッセージングサービス（SMS、Skype、Slack、Line、･･･）
	リアルタイム通信 (VoIP 等)	・SIP★ ・RTP★ ・SRTP
	ファイル共有	・SMB ・CIFS ・WebDAV
	ファイル転送	・SFTP ・FTPS ・FTP★
	リモート接続	・SSH ・RDP ・telnet★
	VPN	・IPsec-VPN ・TLS-VPN
		・IPsec-VPN
		・TLS-VPN

設定／運用	デバイス認証	・クライアント証明書 ・TPM を利用した認証 ・ISO/IEC9798	設定／運用	仮想通貨	・Bitcoin プロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）
	デバイス認証	・Apple MDM ・MS ライセンス認証 ・PUF を利用した認証		放送暗号	・DRM ・ARIB ・W-CDMA

（STEP2）運用ガイドラインを作る価値がある／必要性が高いと判断したものを抽出

表 5 に挙げた暗号プロトコルのうち、運用ガイドラインを作る価値があるか／必要性が高いかを判断するために、以下の観点から整理を行った。その結果、「必要性」「目的・内容」「想定読者」の 3 点について明確に説明できるものを「運用ガイドラインを作る価値がある／必要性が高い」と判断・抽出し（表 3 内の網掛け部分）、より詳細な検討を加えた。

- 【必要性】
  運用ガイドラインを作る価値／必要性を明確に示すことができるか（なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか）
- 【目的・内容】
  どのような目的・内容をもった運用ガイドラインを意図したものかを明確に示すことができるか（3.1 で挙げた目的の 1. ～4. のどれに当たるかが明確であるか）
- 【想定読者】
  その運用ガイドラインの想定読者を具体的に示すことができるか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

表 6 に検討結果をまとめる。今後、暗号プロトコルに関する運用ガイドラインを作成していく際には、表 6 に挙げたもののなかから優先的に取り上げていくことが望ましい。なお、「課題」には CRYPTREC が作成する運用ガイドラインの価値を高めるために考慮しなければならないポイントをまとめており、また「関連組織」には連携先として有効と期待される国内組織（国際組織の日本支部を含む）を記した。活動計画の立案に当たっては、これらのポイントを踏まえた計画であることが望まれる。

なお、表 6 の「目的」列、及び「プロトコル名称」列の表記についての注意は次のとおりである。

「目的」の表記

①・・・現在利用されている仕組みの中で安全ではない使われ方を排除し、安全性の底上げを図る（安全性評価を含む）

②・・・利用者が理解しやすく、かつ採用しやすいベストプラクティスを示す

③・・・普及が進んでいない安全な仕組みの普及・活用を促進させる

④・・・政府、業界団体等が守るべき（半）強制的基準として示す（そうなるような環境整備を含む）

「プロトコル名称」の表記

・「★」がついているプロトコルは暗号に直接関係がないものを指す

・具体的なプロトコル名称がわからないものについては規格やサービスの名称を示す

表 6　取りまとめ結果一覧

種類	No	対象	プロトコル名称	目的	内容	想定読者	必要性	課題	他組織が発行したガイドライン等	関連組織
安全性評価（暗号技術評価委員会への参考意見）	1	ID 連携	OpenID Connect	①	OpenID Connect の安全性評価	（議論せず）	・OpenID Connect は安全性が評価されていないため、CRYPTREC で安全性評価できるとよい。	・OpenID Connect は暗号プロトコルというよりは枠のようなもので、組み合わせで安全性は当然変わる。	（議論せず）	一般社団法人 OpenID ファウンデーション・ジャパン
	2	無線通信	LoRaWAN	①	LoRa で利用されているプロトコルの安全性評価	（議論せず）	（議論せず）	・業界団体に加入していなければ、仕様を見ることができない。	（議論せず）	（議論せず）
	3	仮想通貨	・Bitcoin プロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）	①	ブロックチェーンの安全性評価	（議論せず）	（議論せず）	・標準化が行われている最中であるため、時期尚早。	（議論せず）	（議論せず）

実装／開発	1	自動車	【車内】 CAN, CAN FD, LIN, FlexRay 【車外】 DSRC, ETC2.0 【ハードウェア】 EVITA 【センサ】 空気圧センサ、ミリ波レーダー	②	自動車の中で利用されている暗号の実装ガイドライン（検証方法含む）	自動車ベンダ、部品サプライヤ	・今後の自動運転車などを見据えた際、セキュリティに問題が発生した場合、社会的に大きな問題となることが想定されるため。	・標準化が行われている最中である。 ・規模が大きくCRYPTREC のリソースで対応できる範囲は限られる。 ・プロトコルで挙がっているものを、より細分化し優先順位を付ける必要がある。 ・自動車ベンダの協力が必要である。 ・国内では自動車工業会（JAMA）と連携するか、二人三脚で進めないと作っても受け入れられない懸念あり。 ・自動車業界は、まず欧米の評価を参考とするため、CRYPTREC がガイドラインを作成する場合には自動車業界に受け入れてもらえるような工夫が必要である。 ・DSRC,ETC2.0 のセキュリティを管理するのは ITS-TEA であり、ガイドラインを作成する場合、こことコンタクトする必要があるかもしれない。 ・SHE（Secure Hardware Extension）のように仕様が一般公開されないものに対して CRYPTREC がガイドラインを作るべきかは議論する必要がある。	・SAE j3061：Cybersecurity Guidebook for Cyber-Physical Vehicle Systems ・Cybersecurity Best Practices for Modern Vehicles – NHTSA ・Automotive Cybersecurity Best Practices – Auto ISAC	・JSAE ・JasPar

	2	制御システム	・PLC ・SCADA ・BACKnet, OPC 等	①②	制御システムの中で利用されている暗号プロトコルの実装ガイドライン	システム開発者、運用者	・制御系システムで利用されているソフトウエアに脆弱性が発見された場合は、生命・身体や重要インフラおよび環境へ直接影響を与える可能性があり、重要な問題となりうる。	・PLC、SCADA と挙げているがプロトコル名称ではない。プロトコルは沢山あり、安全性を挙げるために色々なガイドラインを作る必要はあるが沢山あり過ぎて、まずどれから手を付けていいかわからない。他組織との連携も考える必要がある。	・JPCERT/CC のガイドライン、参考資料	・JPCERT/CC https://www.jpcert.or.jp/ics/ ・CSSC
設定／運用	1	ユーザ管理	・RADIUS (EAP-TLS 等の利用を含む) ・PAP★ ・CHAPv2 ・IEEE802.1X	①②	・Radius＋EAP の推奨 ・Radius＋(PAP or CHAPv2)の非推奨 ・PAP、CHAPv2 の非推奨 ・Radius の設定	システム開発者、運用者(ユーザ管理者)、SIer、VPN を使う企業よりのベンダ	・無線 LAN 環境は利用者が多く、また、オリンピックに向けて、アクセスポイント(AP)の設置が増えていくため。 ・公衆無線 LAN 利用者が年々増加しており、3,532 万人を突破している((株)ICT 総研調べ)。 ・VPN のユーザ認証に使われている。	・想定読者を誰にするかによって、対象とする技術が変わる(企業向けにするのであれば RADIUS 認証を利用する)。 ・ユーザが「野良 AP」にアクセスしないように促すことも検討が必要。	・無線 LAN ビジネスガイドライン ・SP 800-48 Rev. 1 Guide to Securing Legacy IEEE 802.11 Wireless Networks ・SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	総務省

設定／運用	2	ユーザ管理	LDAP★ (kerberos)	①②	LDAP＋Kerberos の設定	システム開発者、運用者(ユーザー管理者)、SIer	・Active Directory をはじめとしてディレクトリサービスは企業の ID 管理として利用されているが、特に標的型攻撃で侵入される糸口となるケースが昨今急増している。 ・Windows の Active Directory は広く使われている技術である。 ・組織内データのうち最も狙われやすい情報であり、内部犯行やマルウエア発動による中からの攻撃にも対処する必要がある。	・CRYPTREC で扱う内容であるのかというと疑問、そしてプロトコルの設定として変更できるものはなく、全体的に AD の安全性の設定やシステム設計思想が含まれる内容となると考えられる。 ・主に Kerberos の設定ガイドになりそうである。 ・LDAP に関わる認証方式として Kerberos 以外の実装や運用に関して調査する必要がある。 ・Windows サーバの設定も含まれる。	・Active Directory のセキュリティを保護するためのベスト プラクティス (MS) ・攻撃に対する保護のドメインコントローラ(MS) ・PtH(Pass-the-Hash) White Papers and Data Sheet (MS) ・『LDAP 認証と Azure Multi-Factor Authentication Server』 ・『RFC2251 Lightweight Directory Access Protocol (v3)』	各種 LDAP 製品ベンダ (MS, Oracle, IBM など)

設定／運用	3	ユーザ認証	・二要素認証	①②	・パスワード管理のガイドライン（パスワード管理の一環として二要素認証を位置付ける形）	・サービサー、SIer、IDプロバイダ	・クラウドやバンキングなどで二要素認証の利用が増加しているが適切に管理できていないケースがある。 ・金銭や証券だけでなく、ポイント・アイテムの管理に利用されているため安全なログイン環境が必要である。	・かつてRFC化（RFC2289）されているがMD4ベースであり脆弱である。それ以降のOTPはRFC4226 HMAC-BasedOTP, RFC6238 Time-BasedOTPが標準化されているが利用状況は不明であり、Proprietaryなシステムもあると考えられる（＝調査不能）。 ・OTP自体はプロトコルではない。OTPの生成方法は本WGの対象ではない。	・（パスワードに関するガイドラインで触れられているかもしれないが、現時点ではOTPに関するガイドラインは見つけられず） ・医療システムの安全管理に関するガイドライン（厚生労働省） ・オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン	銀行、オンラインゲームサービス企業、SIer
	4	デバイス認証	・クライアント証明書 ・TPMを利用した認証 ・ISO/IEC 9798	①②	・クライアント証明書やTPMを使った実際のデバイス認証のガイドライン ・相互認証等の規格（ISO/IEC979	・システム開発者、運用者	・IoT機器なども含め、ネットワーク接続機器が大きく増える見込みの中、デバイスレベルでの認証は安全性確保のため極めて有効である。 ・広く利用されつつあるデバイス認証のセキュリティを強化するため。 ・利用が増えているが、適切な管理などに明るくない管理者が多い。 ・社内もしくは組込み機器等でネットワ	・Proprietaryなシステムが多く標準化文書はない可能性が高い。また仕様の入手が困難かもしれない。 ・幅広い技術があるので、対象を絞る必要があるか。 ・「暗号プロトコル」に整理できない技術も含まれる。	・TCGアライアンス発行の文書等 ・ISO/IEC9798	TCGアライアンス

					8)が定めているパラメータの選定方法や利用方法の具体化、設計時の指針		ークに接続する機器が増え、IT 系と同様の対策を講じる際に、設計者、開発者の指針になる文書があるとネットワークを構築する際に参考になる。				
設定／運用	5	無線通信	・WEP ・WPA ・WPA2	①②	・WEP の非推奨 ・WPA、WPA2 の設定	・企業等での無線 LAN の管理者（企業で簡易に無線 LAN を設定する人） ・一般家庭等での無線 LAN の利用者（一般家庭等で無線 LAN を利用する人） ・IoT で Wi-Fi の利用者	・3DS が WEP しか対応されていないことなど利便性を考慮して脆弱な古いプロトコルが未だに利用されていると考えられる。それを排除する必要がある。 ・無線 LAN の設置が増えているため。	・想定読者を誰にするかによって、対象とする技術が変わる（企業向けにするのであれば RADIUS 認証を利用する）。 ・ユーザが「野良 AP」にアクセスしないように促すことも検討が必要。 ・発言力のある人が言うレベルになっているのではないか。	・無線 LAN〈危険回避〉対策のしおり ・SP 800-48 Rev. 1 Guide to Securing Legacy IEEE 802.11 Wireless Networks ・SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i ・無線 LAN ビジネスガイドライン（総	総務省

									務省） ・一般家庭における無線 LAN のセキュリティに関する注意	
設定／運用	6	メール	・DKIM ・SPF★ ・DMARC★	②③	DMARC（SPF と DKIM を含む）の設定/普及	メールサーバを構築するシステム開発者、運用者	・メール送信ドメインのなりすまし対策として必要。 ・SPF、DKIM、DMARC を全て合わせて使うことを普及すべき。	・ガイドラインを書くにあたっての課題は特段ない。 ・迷惑メール対策推進協議会、および迷惑メール対策委員会と同期を取って、普及することが望ましい。	・dkim.jp リコメンド文書 ・電子メールのセキュリティ ・標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果 ・ 府省庁対策基準策定のためのガイドライン（平成 28 年度版）(NISC) ・フィッシング対策ガイドライン(フィッシング対策協議会) ・迷惑メール対策ハンドブック 2016	・JIPDEC ・迷惑メール対策推進協議会(事務局:デ協) ・迷惑メール対策委員会（事務局:IAJapan)

									（迷惑メール対策推進協議会） ・「有害情報対策ポータルサイト－迷惑メール対策編－」（迷惑メール対策委員会）	
設定／運用	7	メール	S/MIMEを利用したメール送信（メールへの署名）	②③	S/MIMEの設定／普及	メールサーバを構築するシステム開発者、運用者、メール送受信者	・メールのなりすまし対策として必要。 ・現在未対応のWebメールやスマホのメーラに対応を促したい（Office365やGmailは一部対応済）。 ・なりすまし対策としてS/MIMEが（特に署名で）使われ始めているが、メーラごとに癖があり設定の方法がわかりにくい。 ・フィッシング対策として銀行や大手プロバイダがS/MIMEを導入する傾向にある。	・ガイドラインを書くにあたっての課題は特段ない。 ・Googleの新システムでは秘密鍵をクラウド上で管理するようであり、これまでこの手のガイドラインでは想定していなかった使われ方がなされることも視野に入れる必要があるかもしれない。	・SP 800-45 Version 2 Guidelines on Electronic Mail Security ・SP 800-177 Trustworthy Email ・標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果 ・ 府省庁対策基準策定のためのガイドライン（平成28年度版）（NISC）	・総務省 ・JIPDEC ・フィッシング対策協議会 ・IPA

									・フィッシング対策ガイドライン（フィッシング対策協議会） ・電子メールのセキュリティ（IPA）	
設定／運用	8	メール	・パスワードつきZipを添付したメール送信 ・S/MIMEを利用したメール送信（メールの暗号化） ・オンラインストレージサービス	①②③	・パスワード付きzip添付メールの排除 ・S/MIMEの設定／普及 ・オンラインストレージサービスの使い方の解説	メールサーバを構築するシステム開発者、運用者、メール送受信者	・メールの秘匿性を高めるため。 ・パスワード付きzipファイルのメール送信をやめることで、受信サイドの業務効率の向上と受信サイドのセキュリティ強化。 ・現在未対応のWebメールやスマホのメーラに対応を促したい（Office365やGmailは一部対応済）。	・ガイドラインを書くにあたっての課題は特段ない。 ・オンラインストレージサービスは様々あり、少々書きにくい面はある。 ・Googleの新システムでは秘密鍵をクラウド上で管理するようであり、これまでこの手のガイドラインでは想定していなかった使われ方がなされることも視野に入れる必要があるかもしれない。 ・政府系向けのガイドラインでは、組織間の暗号化のように、組織のどこかで責任をもって、一旦、暗号化を外して中を見る等を考慮したガイドラインが必要となるかもしれない。	・SP 800-45 Version 2 Guidelines on Electronic Mail Security ・SP 800-177 Trustworthy Email ・ 府省庁対策基準策定のためのガイドライン（平成28年度版）（NISC） ・電子メールのセキュリティ（IPA）	・JIPDEC

設定／運用	9	リモート接続	・SSH ・RDP ・telnet★	①②	・telnet の非推奨 ・SSH の設定 ・RDP の設定	・企業等でサーバにリモート接続するシステム運用者 ・リモートデスクトップ接続を行うシステムを構築しているシステム管理者、運用者	・SIer のほとんどが SSH を利用しているため、SSH は必要。 ・IoT でも SSH は広く利用されるため。 ・IPsec や SSH のガイドラインはリファレンスとして出せれば役に立つ。 ・Web ホスティングサービスでは SSH サービスを開放しているケースもあり、想定読者はエンジニアだけではなく一般ユーザにも拡大される可能性がある。 ・パラメータが多い為、SSH サーバの設定によっては非常に危険な状態になる。特に特権ユーザのパスワードログインを可能にしている場合は注意が必要。 ・RDP は、クラウド上でも利用されていて、設定が悪いと世界中誰からも乗っ取られて利用される恐れがあるため。	・他組織との連携（例. 他組織で作成済みのガイドラインを取り込む）が必要。	・SSH サーバセキュリティ設定ガイド Ver 1.0 ・SP 800-46 Rev. 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	日本シーサート協議会

3.2. 運用ガイドラインのアップデート方法に関連する検討

運用ガイドラインは、ガイドライン作成時の標準化状況や製品状況、利用環境や利用実績等を踏まえて、作成時における現実的かつ効果的な推奨設定や推奨基準を提示するものである。このことは、ある程度の時間が経過し、標準化状況や製品状況、利用環境や利用実績等が変化すれば、運用ガイドラインの中身も陳腐化し、ガイドラインとしてふさわしくないものとなることを意味する。

このため、今後運用ガイドラインの整備を進めるにあたっては、単に運用ガイドラインを作るだけでなく、運用ガイドラインの質を維持するためにどのような方法でアップデートを行っていくかを検討しておく必要がある。そこで、活用委員会では、具体的な運用ガイドラインの例として「SSL/TLS 暗号設定ガイドライン」を取り上げ、アップデートの在り方の検討を行った。

一般的なアップデートの方向性について

- 見直しの期限を設定（定期的なアップデートの実施是非）について：
  ガイドラインの内容自体のアップデート（内容をどのように改訂するか）とガイドラインのステータス管理（アップデートを実施するか否かの判断）を切り分けて考える。具体的には、ステータス管理については定期的に行うが、内容の改訂を行う期限自体はあらかじめ決めておかない。
  なお、ステータス管理ではアップデートを実施するか否かだけを決めることとし、実際の内容の改訂はアップデートすることが決まった後に実施する。

- アップデート方法について：
  毎回本体のアップデートを行うのではなく、注釈を加える程度であれば比較的負荷は掛からないため、必要に応じて注釈を後ろに付け加えていくやり方もある。例えば 2～5 年経過して、注釈が溜まってきたら大きなバージョンアップをして、内容を大幅に改訂する。
  また、緊急に対応すべき情報（補足情報）は、少なくとも運用ガイドラインと併せてインターネット上で入手できるようにすべき。本体と補足情報を合わせて同時に参照することにより対策を打つことができる。

「SSL/TLS 暗号設定ガイドライン」に関してのアップデートの方向性について

- どこまでの内容をアップデートすべきか（次回アップデートの範囲）：
  IETF では、RC4 の使用禁止、SSL3.0 の非推奨、TripleDES の非推奨等の RFC を発行しており、2015 年の「SSL/TLS 暗号設定ガイドライン」発行時とは劇的に状況が変わっている。実際、認定認証事業者が発行する証明書では SHA256 へ

の移行が完了し、パブリック証明書もほぼ SHA256 with RSA2048 ビットになっている。また、2015 年には問題になっていたフィーチャーフォンについてもキャリアが SHA1 証明書での接続はできないと注意喚起しているはずであるため、必ずしもセキュリティ例外型が必要とは言えなくなってきている。
したがって、早期に最新動向の反映、及びセキュリティ例外型の見直しまで含めて、内容の改訂を実施すべきである。
一方、各社の製品の設定は徐々に各社で作るようになっていくべきであるため、市販製品の暗号設定状況の調査結果及び Appendix に乗っている OSS 製品等の暗号設定状況については、ガイドラインから分離すべきである。また、各社の製品の設定例を各社で整備するようにアピールをすべきである。

- セキュリティ例外型の利用を終了させる時期（EOL）の導入是非について：
  EOL を導入することで、EOL までは利用を容認すると誤解される恐れがあるため、セキュリティ例外型について EOL を導入すべきではない。また将来的には、現在の推奨セキュリティ型からセキュリティ例外型に移す必要がある設定が出てくる可能性を踏まえれば、セキュリティ例外型の枠を無くさないほうが望ましい。

3.3. 外部連携について

運用ガイドラインの作成については、CRYPTREC 単独で作成するよりも関連する外部組織や業界団体等（以降、他組織等という）との連携を進めたほうがよいとの指摘があった。例えば、以下のような指摘である。

- 暗号プロトコル課題検討 WG の検討結果では、必要性が高いと認められた暗号プロトコルはいずれも、外部組織や業界団体との連携するほうが、効果が高い運用ガイドラインが作れると考えられる。
- 重点課題検討 TF での議論の中では、従来は民間が必要としていた情報と電子政府を作るうえで必要となる情報の方向性がほぼ一致していたが、現在はそうでないという指摘があった。
- ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保することが効果的なガイドラインとして評価される。

これらの指摘を踏まえ、来年度より開始する運用ガイドラインの作成にあたっては、従来の WG 形式での作成に捕らわれずに柔軟な作成スタイルを考慮する。具体的には、運用ガイドラインの作成手段を次の 4 種類とし（図 3 参照）、作成するガイドラインのテーマによって、暗号技術活用委員会にて適切な作成手段を決定する。

1) CRYPTREC が単独で作成（2 種類）

CRYPTREC が他組織等と連携なしに単独で作成する。ただし、具体的な作成手段としては、従来の WG 形式のほか、スキルのある他組織等にアウトソーシングしてベースとなる素案を作成してもらい活用委員会で内容を確認・承認する形式も含める。

2) 他組織等と共同で作成

他組織等と共同で作成したものを活用委員会で確認・承認する形式である。

3) 他組織等で実施したものをベースに作成

他組織等がすでに作成したものをベースに委員会で確認し、適切なものであれば承認する形式。その際、他組織がすでに作成したものを参照したうえで、必要最小限の追記等を行う可能性がある。

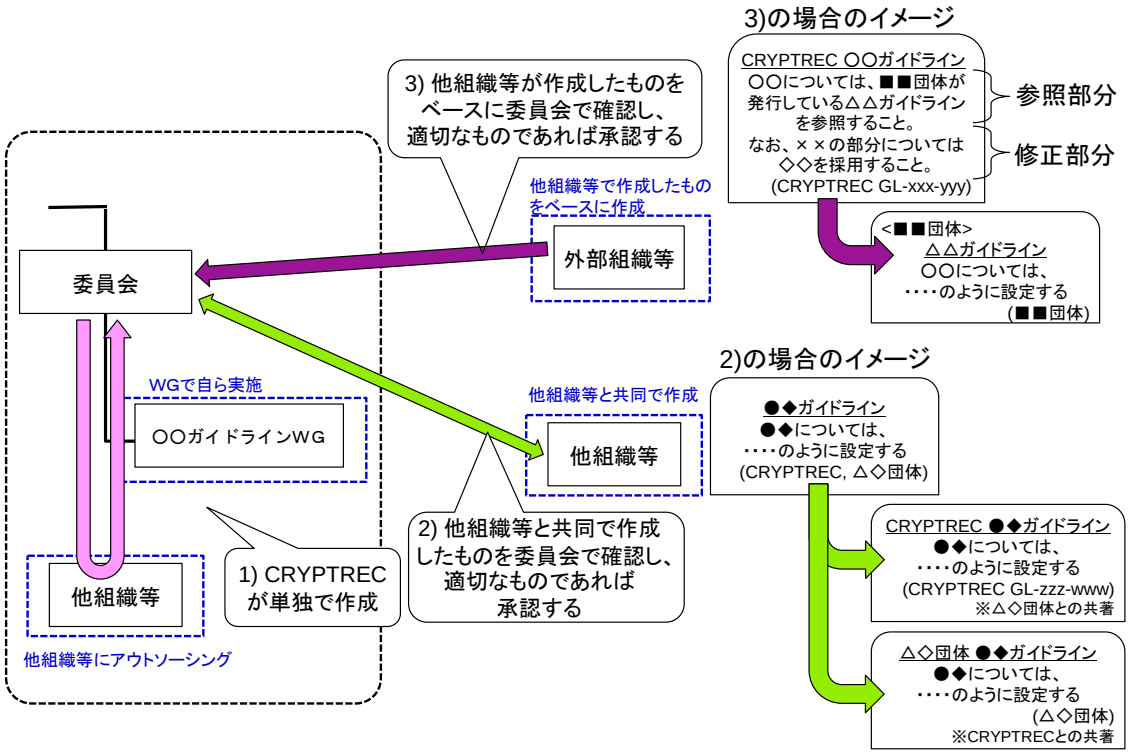

図 3　作成手段の説明図

実際の運用ガイドラインの作成手段を決定するにあたっては、以下のポイントを重視して判断を行う。

- 他組織等と連携するほうが有用性のある運用ガイドラインが作成できるか

- 連携先の外部組織等が信頼できる組織・団体であるか
- 他組織等と連携することによって作業効率を上げることができるか（例えば作業スケジュール等）
- 予算面やリソース面からの考慮

4. 今後に向けて

2017 年度は新たな運用ガイドラインを実際に作成していく方向で活動計画を検討する。具体的な対象の選定等については、2017 年度第一回暗号技術活用委員会にて決定する方向である。

また、SSL/TLS 暗号設定ガイドラインについては、2016 年度活動で出た意見を踏まえ、2017 年度にアップデートを行う計画とする予定である。

CRYPTREC Report 2016
(暗号技術活用委員会報告　CRYPTREC-RP-0003-2016)

発行日　2017年6月30日 第1版
発行者
・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人 情報処理推進機構
(技術本部 セキュリティセンター 暗号グループ)
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北町四丁目2番1号
国立研究開発法人 情報通信研究機構
(サイバーセキュリティ研究所 セキュリティ基盤研究室)
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN